HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

الجريمة السيبرانية بين السياسات الوطنية والمنظمات العقابية

أحمد عبد الرضا حمزة غزالي[1]

[1] الجامعة الإسلامية في لبنان.

اشراف: الأستاذ الدكتور محمد منذر/ تدريسي في الجامعة الإسلامية في بيروت

HNSJ, 2026, 7(5); https://doi.org/10.53796/hnsj75/64

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/75/64

تاريخ الاستقبال: 2026/04/15م تاريخ القبول: 2026/04/22م تاريخ النشر: 2026/05/01م

المستخلص

تهدف هذه الدراسة إلى بيان طبيعة الجريمة السيبرانية بوصفها إحدى أبرز صور الإجرام المستحدث في البيئة الرقمية، وتحليل مدى كفاءة السياسات الوطنية والمنظومات العقابية في مواجهتها، في ظل ما تتسم به هذه الجرائم من سرعة في التنفيذ، وصعوبة في الكشف والإثبات، وطابع عابر للحدود. وتكمن أهمية الدراسة في أن الجرائم السيبرانية لم تعد أفعالاً فردية محدودة، بل أصبحت ظاهرة منظمة تهدد الأمن القانوني والاقتصادي والاجتماعي للدول، الأمر الذي يفرض ضرورة تطوير التشريعات الوطنية، وتعزيز القدرات الفنية للأجهزة الأمنية والقضائية، وتفعيل التعاون الدولي في مجالات تبادل المعلومات، والمساعدة القانونية، وتسليم المجرمين، وحفظ الأدلة الرقمية. وقد اعتمدت الدراسة المنهج التحليلي من خلال تناول الخطط الوطنية للحد من الجرائم السيبرانية، والإجراءات الفنية والتشريعية لمواجهتها، مع الوقوف على نماذج من التشريعات العربية والأجنبية ومدى انسجامها مع قواعد القانون الجنائي الدولي. وتوصلت الدراسة إلى أن السياسات الوطنية، رغم أهميتها، تظل محدودة الفاعلية إذا لم تتكامل مع الجهود الدولية، كما أن قصور التشريعات، وتعدد الاختصاصات القضائية، وصعوبات الإثبات الرقمي، تمثل تحديات رئيسية أمام تحقيق الردع الجنائي الفعال. وخلصت الدراسة إلى ضرورة اعتماد مقاربة شاملة تقوم على تحديث القوانين، وإنشاء وحدات متخصصة، وتطوير آليات الإثبات الرقمي، وتعزيز التعاون الدولي، ونشر الوعي المجتمعي، بما يحقق توازناً بين حماية الأمن السيبراني وضمان الحقوق والحريات في الفضاء الرقمي.

الكلمات المفتاحية: الجريمة السيبرانية، السياسات الوطنية، القانون الجنائي الدولي، الإثبات الرقمي، التعاون الدولي.

RESEARCH TITLE

Cybercrime between National Policies and Penal Systems

Abstract

This study aims to examine the nature of cybercrime as one of the most prominent forms of emerging crime in the digital environment, and to analyze the effectiveness of national policies and penal systems in confronting it, particularly in light of the speed with which such crimes are committed, the difficulty of detecting and proving them, and their transnational nature. The significance of the study lies in the fact that cybercrime is no longer limited to isolated individual acts; rather, it has become an organized phenomenon that threatens the legal, economic, and social security of states. This requires the development of national legislation, the enhancement of the technical capacities of security and judicial authorities, and the activation of international cooperation in the areas of information exchange, legal assistance, extradition, and the preservation of digital evidence. The study adopts the analytical method by examining national plans to reduce cybercrime, as well as the technical and legislative measures used to combat it, while reviewing examples of Arab and foreign legislation and the extent of their compatibility with the rules of international criminal law. The study concludes that national policies, despite their importance, remain limited in effectiveness unless they are integrated with international efforts. It also finds that legislative shortcomings, jurisdictional conflicts, and difficulties related to digital evidence constitute major challenges to achieving effective criminal deterrence. The study ultimately recommends adopting a comprehensive approach based on updating laws, establishing specialized units, developing mechanisms for digital evidence, strengthening international cooperation, and raising public awareness, in a manner that ensures a balance between protecting cybersecurity and safeguarding rights and freedoms in the digital space.

Key Words: Cybercrime, national policies, international criminal law, digital evidence, international cooperation.

المقدمة

تعد جرائم الإنترنت والجرائم السيبرانية من أكثر الجرائم التي أصبحت تشكل تهديداً كبيراً في العصر الحديث من خلال الأنشطة غير القانونية التي تستهدف أنظمة المعلومات والشبكات الإلكترونية يهدف الوصول غير المصرح به للتلاعب بالبيانات أو للاحتيال الإلكتروني والتجسس وغيرها من الأنشطة الضارة لذلك يجب تعزيز السياسات والتشريعات إنشاء قوانين ولوائح تحد من الأنشطة السيبرانية الضارة لحماية الأفراد والشركات، التي يجب أن تكون هذه السياسات محدثة ومتناسقة مع التطورات التكنولوجية الجديدة كما يجب اعتبار الجرائم السيبرانية مسألة دولية، تهدف لتعزيز التعاون بين الحكومات والوكالات الإنفاذية والقطاع الخاص عبر الحدود لمكافحة هذه الجرائم.

لذلك فقد سنت العديد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت بعض البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت أما على مستوى الدول العربية فلم تقم أي دولة عربية بسن قوانين خاصة بجرائم الحاسب الآلي والانترنت، إلا أن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية التي تفرض نوعاً من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية واتخاذ إجراءات فورية تجاه المخالفين في المواقع الالكترونية حيث يتم تدميرها إذا ثبت أنها أوقعت أضرار بمصلحة الأمن القومي أو بالآداب العامة[1]، لهذا دعت الحاجة إلى تطوير التشريعات الموجودة حاليا بما يواكب التطور العلمي والتكنولوجي بما يكفل حقوق المواطنين المستخدمين شبكة المعلومات الدولية، وتحدد واجباتهم.

أولاً_ أهمية البحث

تنبع أهمية الدراسة من التحولات العميقة التي فرضها التطور التكنولوجي المتسارع، والذي أدى إلى بروز أنماط جديدة من الجرائم تتجاوز الحدود الجغرافية للدول وتستهدف الأفراد والمؤسسات على حد سواء، فالجريمة السيبرانية لم تعد مجرد أفعال معزولة، بل أصبحت ظاهرة منظمة تتسم بالتعقيد والتطور المستمر الأمر الذي يفرض على الدول إعادة النظر في سياساتها الجنائية والتشريعية لمواكبة هذه التحديات.

ثانياً_ أهداف البحث

تهدف هذه الدراسة إلى تحقيق جملة من الغايات العلمية والعملية، أبرزها تحليل مفهوم الجريمة السيبرانية وخصائصها المميزة، وبيان طبيعة التحديات التي تفرضها على الأنظمة القانونية التقليدية. كما تسعى إلى تقييم السياسات الوطنية المعتمدة في مكافحة هذه الجرائم، ومدى فعاليتها في الردع والمعالجة.

ثالثاً_ إشكالية البحث

تتمحور إشكالية الدراسة حول مدى كفاءة وفعالية السياسات الوطنية والمنظمات العقابية في مواجهة الجريمة السيبرانية في ظل الطبيعة العابرة للحدود لهذه الجرائم والتطور المستمر في وسائل ارتكابها، إذ تثير هذه الظاهرة تساؤلات جوهرية تتعلق بمدى قدرة التشريعات الوطنية على مواكبة هذا التطور، ومدى انسجامها مع الجهود الدولية فضلاً عن إشكالية الاختصاص القضائي وصعوبة تعقب الجناة، وتحديات الإثبات الرقمي، ومن ثم يمكن صياغة الإشكالية في تساؤل رئيسي مفاده: **إلى أي مدى تنجح السياسات الوطنية والمنظمات العقابية في تحقيق استجابة فعالة ومتوازنة لمواجهة الجريمة السيبرانية في ظل التحديات القانونية والتقنية المعاصرة؟**

---

[1] أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، مصر، 2008، ص80.

رابعاً_ منهجية البحث

تعتمد هذه الدراسة على المنهج التحليلي من خلال تحليل النصوص القانونية الوطنية والدولية ذات الصلة بالجريمة السيبرانية، وبيان مدى كفايتها في مواجهة هذه الظاهرة.

خامساً_ خطة البحث

المطلب الأول: الخطط الوطنية للحد من الجرائم السيبرانية.

الفرع الأول: مواجهة الإرهاب السيبراني.

الفرع الثاني: الاجراءات الفنية لمواجهة الجرائم السيبرانية.

المطلب الثاني: الجريمة السيبرانية بين التشريعات الجنائية والقواعد الجنائية الدولية.

الفرع الأول: انسجام القوانين الجنائية في الدول العربية مع المعايير الجنائية الدولية.

الفرع الثاني: توافق النظم العقابية في التشريعات الأجنبية مع قواعد القانون الجنائي الدولي.

المطلب الأول

الخطط الوطنية للحد من الجرائم السيبرانية

يعيش اليوم العصر الرقمي بفضل الثورة الهائلة في تكنولوجيا المعلومات والاتصال، فزيادة التشابك في جميع المجالات أدى إلى خلق بيئة جديدة للتفاعل بين الأفراد والمجتمعات والدول، وهو ما اصطلح عليه بالفضاء السيبراني هذا الفضاء الذي يتميز بالتطور السريع، والغموض الشديد، كما خلق الاستخدام السيئ لهذا الفضاء بيئة مليئة بالمخاطر والتهديدات، شكلت تهديداً خطيراً للأمن القومي للدول حيث سارعت هذه الدول لتشكيل الهيئات والمؤسسات المدنية والعسكرية، وسنّ التشريعات القانونية ووضع استراتيجية خاصة لمواجهة التهديدات السيبرانية الحالية والمستقبلية والدفاع عن أمنها، فضلاً عن العمل على المستويين الإقليمي والدولي من أجل فضاء سيبراني أمن وسلمي[2]، **فبناءً على ذلك سوف نقسم هذا المطلب إلى فرعين، سنتناول في الفرع الأول مواجهة الإرهاب السيبراني، وفي الفرع الثاني سنتناول الاجراءات الفنية لمواجهة الجرائم السيبرانية.**

الفرع الأول

مواجهة الإرهاب السيبراني

هناك تحديات لمساعي مواجهة الإرهاب السيبراني، يتعلق كثير منها بالتطورات السريعة والمتلاحقة في مجال التقنية الالكترونية، وتطور برامج التخفي وعزل تقنيات التتبع، وتقدم برامج تغيير المواقع، لذا يمكن ترتيب سُبل مواجهة هذا النمط من الإرهاب وفق الاجراءات السياسية والتدابير التنظيمية الآتية [3]:

1-**السياسات السيبرانية:** إن سياسة الدولة على المستويين المحلي والدولي تحدد توجهاتها في الفضاء السيبراني، ويبدو أن بعض الدول الكبرى الناشطة في الفضاء الإلكتروني مثل الصين وروسيا لديها تحفظات تتعلق بهذا الفضاء، إذ رأت كل منهما في العولمة السيبرانية تعدياً على سيادة الدولة القومية، ولا يمكن لأي دولة في ظلها أن تسيطر على المضمون

[2] حامد محمد علي البلداوي، الهجمات السيبرانية أضرارها وآثارها ومواجهتها في قواعد القانون الدولي الإنساني، المركز العربي، القاهرة، 2024، ص115.

[3] حامد محمد علي البلداوي، الهجمات السيبرانية أضرارها وآثارها ومواجهاتها في قواعد القانون الدولي الإنساني، مرجع سابق، ص133.

المتداول بين مواطنيها عبر شبكة الإنترنت، لذلك أقامت كل منهما الحواجز اللازمة وأنشأت شبكاتها القومية الخاصة ضمن إطار شبكة الإنترنت العالمية، وبحسب ضوابطها الخاصة، ونجحت كلا الدولتين في تحقيق ذلك، فضلاً عن تبني معظم الدول الكبرى الذباب الإلكتروني[4].

2- **تبادل التعاون لمواجهة الكوارث والأزمات والمواقف الحرجة:** يعد عنصر الوقت من المحددات الجوهرية في فاعلية التصدي للهجمات السيبرانية، إذ تفرض طبيعة هذه الجرائم سرعةً فائقة في التنفيذ وصعوبةً في التتبع، الأمر الذي يجعل من التعاون الدولي في إطار القانون الجنائي الدولي ضرورة حتمية وليست خياراً، فهذه الجرائم تتجاوز الحدود الجغرافية والسيادية للدول وتستلزم استجابةً منسقة تقوم على تبادل المعلومات والخبرات والوسائل التقنية في أقصر وقت ممكن، مما يعزز قدرة المجتمع الدولي على احتواء الخطر ومنع تفاقمه[5].

إن تفاوت الإمكانيات التقنية والتشريعية بين الدول، ولا سيما بين الدول المتقدمة والنامية، يخلق فجوة قانونية وأمنية يستغلها مرتكبو الجرائم السيبرانية للانتقال من دولة إلى أخرى أو لإخفاء آثارهم ضمن أنظمة قانونية ضعيفة أو بطيئة الاستجابة، ومن هنا تتجلى أهمية القانون الجنائي الدولي في إرساء قواعد ملزمة للتعاون القضائي والأمني، تتيح تبادل الأدلة الرقمية، وتسليم المجرمين، وتوحيد أسس التجريم والعقاب، كما أن الاتفاقيات الدولية مثل اتفاقية بودابست لعام 2001 بشأن الجريمة السيبرانية، تعد نموذجاً عملياً لتفعيل التعاون الدولي في المجال الجنائي الإلكتروني، إذ تهدف إلى توحيد التشريعات الوطنية وتسهيل تبادل المعلومات بين أجهزة إنفاذ القانون في الدول الأطراف، وفي هذا السياق لايقتصر دور القانون الجنائي الدولي على تجريم الأفعال، بل يمتد إلى بناء إطار مؤسسي للتعاون الوقائي عبر التدريب والتأهيل ورفع الكفاءة التقنية لرجال العدالة والشرطة في مواجهة الجرائم المستحدثة.

3- **الجوانب التنظيمية والتشريعية** تعد التشريعات القانونية الوطنية والدولية الركيزة الأساسية في بناء منظومة فعالة لمواجهة الإرهاب والجريمة السيبرانية، إذ لايمكن تحقيق الردع أو العدالة دون وجود قواعد قانونية موضوعية وشكلية متكاملة تراعي خصوصية الفضاء الرقمي، فالقانون الجنائي الدولي من خلال مبادئه واتفاقياته متعددة الأطراف، يسعى إلى دعم الدول في تطوير تشريعاتها الداخلية بما يتوافق مع المعايير الدولية لمكافحة الجرائم العابرة للحدود ومن بينها الجرائم الإلكترونية[6].

ومن جانب آخر يشجع القانون الجنائي الدولي على إنشاء مؤسسات وطنية متخصصة في مكافحة الجريمة السيبرانية، تتمتع بسلطات تنسيقية وتعاونية مع المنظمات والهيئات الدولية، لضمان سرعة الاستجابة وتعزيز القدرات التقنية والتحقيقية. فالمواجهة الفعالة لمثل هذه الجرائم لا تتحقق إلا من خلال منظومة مؤسسية متكاملة تتعاون في إطار تشريعي منسجم مع المعايير الدولية، بما يحد من فرص الإفلات من العقاب ويعزز الأمن القانوني في الفضاء السيبراني.

4_ الإستراتيجيات السيبرانية: الإستراتيجية السيبرانية للدولة تحدد توجهها في هذا المجال، وتشمل كل السياسات والجوانب الأخرى ذات الصلة مثل المؤسسات المخولة بتنظيم النشاطات الرقمية وضبطها ومواكبة التشريعات للتطور الحاصل في

---

[4] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، مقال منشور بتاريخ 21-1-2021 على الرابط التالي https://www.imctc.org/ar/eLibrary/Articles/Pages/articles2112021.aspx، تاريخ الزيارة 1-4-2026.

[5] أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة أعدت لنيل درجة الدكتوراه في القانون العام، جامعة عين شمس، مصر، 2012، ص 279.

[6] درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني، أطروحة اعدت لنيل درجة الدكتوراه في القانون العام، جامعة أبو بكر، الجزائر، 2017، ص 76.

هذا المجال والاهتمام بتوعية المستخدمين بالمخاطر المحتملة.

5_ الاتفاقيات الإقليمية والتعاون الدولي: تشمل الاتفاقيات الثنائية بين الدول الجوانب القانونية اللازمة للتعاون في مجال التحقيق في حوادث الفضاء الإلكتروني، أما التحالفات السيبرانية بين الدول أو مع القطاع الخاص فهي مهمة في عمليات التتبع والتحقيق في الحوادث، وتبادل المعلومات عن أبرز الطرق الإجرامية المتبعة، وأهم الأختام الرقمية والبصمات الإلكترونية الخاصة بالتنظيمات الإرهابية، وأحدث البرمجيات والأسلحة السيبرانية المستخدمة ما يساعد على تحديد هوية الجهة التي تنفذ الهجمات الإرهابية السيبرانية، ويسهل استهدافها[7].

6-**إنشاء المجلس القومي للمعلوماتية والانترنت:** فالأمن المعلوماتي هو جزء حيوي من الأمن القومي وإن المسؤولية يجب أن يتعاون فيها كل من الجهات التقنية والأمنية والقضائية على أن يكون من ضمن اختصاصاته اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والانترنت وإعداد تقارير إحصائية ومتابعة ما تم عالمياً في هذا المجال[8].

7-**التدابير الأمنية والاستخبارية السيبرانية:** تلعب الجهات الأمنية السيبرانية دوراً محورياً ومتعدد الأوجه في منظومة مكافحة الجريمة الإلكترونية، إذ تتخطى مهماتها مجرد الاستجابة للحوادث لتشمل جملة من الوظائف الوقائية والاستخباراتية والتنسيقية والقانونية، فبصرف النظر عن اسمها المؤسسي (مثل فرق الاستجابة للحوادث الأمنية CSIRT/National CERT) أو وحدات أمن الفضاء الإلكتروني) تعنى هذه الجهات بكشف ثغرات الأنظمة المحلية وتقييم المخاطر التقنية، ووضع تدابير استباقية لتقليل سطح الهجوم، بما يشمل إصدار تحذيرات فنية وتوصيات للتصحيح والتحديث، وإعداد خطط للطوارئ والاستجابة السريعة للحوادث [9].

ومن ناحية التحقيقات الجنائية التقنية فإن هذه الجهات تؤمن إجراءات الأدلة الرقمية (forensics)وفق معايير تحفظ سلاسل الحيازة وتهيئ المواد لإجراءات قضائية لاحقة، كما تتعاون مع جهات إنفاذ القانون المحلية لإجراءات الضبط والتحقيق والتوقيف حين تتوفر دلائل على ارتكاب جرائم سيبرانية، وتبرز هنا صعوبة التعرُّف إلى الفاعل (الإسناد) وحفظ الدليل الرقمي عبر الحدود، ما يجعل التنسيق الدولي وإجراءات التعاون القضائي (MLA، تسليم، تبادل معلومات فنية) أمراً لا غنى عنه لإتمام المتابعات القضائية.

الفرع الثاني

الاجراءات الفنية لمواجهة الجرائم السيبرانية

يظهر تحليل الواقع التقني الحديث أن مرونة الأنظمة الوطنية لم تعد ترفاً تقنياً بل شرطاً جوهرياً للأمن السيبراني العالمي، إذ إن قدرة الدولة على حماية بياناتها ومؤسساتها ترتبط مباشرة بمدى فاعلية منظومتها القانونية والتقنية في مواجهة التهديدات الإلكترونية، فالهجمات المعروفة بهجمات يوم الصفر" تمثل تحدياً خاصاً للمجتمع الدولي، لأنها تقوم على استغلال ثغرات غير مكتشفة في البرمجيات أو الأجهزة، مما يجعلها سابقة لأي تدخل وطني تقليدي.

وفي هذا السياق يبرز دور القانون الجنائي الدولي كإطار للتنسيق والتعاون بين الدول في تبادل المعلومات الاستخباراتية والتقنية المتعلقة بتلك الثغرات، ووضع آليات قانونية ملزمة تجبر الشركات المطوِّرة على الإفصاح السريع عن الثغرات

---

[7] عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص 24-25.

[8] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، المرجع الإلكتروني السابق.

[9] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، المرجع الإلكتروني السابق.

الأمنية وإصدار التصحيحات البرمجية الوقائية، كما يمكن أن يضطلع هذا القانون بوضع معايير دولية لتجريم الأفعال التي تستغل تلك الثغرات، وتحديد المسؤولية الجنائية للأفراد أو الكيانات التي تتعمد استغلالها لتحقيق أغراض ضارة، وتتضمن هذه الاجراءات تطوير البرمجيات والتطبيقات والأدوات والبنية التحتية الإلكترونية للدول لمواجهة الجرائم السيبرانية، وتشمل ما يأتي:

1- تغيير الثقافة وتطوير التفكير السيبراني: يعد نشر التوعية الأمنية بين الأفراد وتطوير قدرات الجهات المختصة من أهم التدابير لمواجهة الجرائم السيبرانية، إذ يعزز التزام المجتمع بالقوانين الوطنية والدولية، ويسهل على الجهات القضائية الدولية متابعة الجرائم وملاحقة مرتكبيها بموجب الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية [(10)].

2- **تغيير الثقافة وتطوير التفكير السيبراني:** يعد نشر التوعية الأمنية بين الأفراد وتطوير قدرات الجهات المختصة من أهم التدابير لمواجهة الجرائم السيبرانية، إذ يعزز التزام المجتمع بالقوانين الوطنية والدولية، ويسهل على الجهات القضائية الدولية متابعة الجرائم وملاحقة مرتكبيها بموجب الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية [(11)].

3-**جدران الحماية (Firewalls) وإجراءات حماية الحسابات:** تعتبر هذه الإجراءات الخط الأول لمنع الوصول غير المشروع للأنظمة، وتساعد في الحفاظ على الأدلة الرقمية ضمن بيئة آمنة، بما يتيح تطبيق العقوبات الجنائية الدولية عند وقوع الاختراق، ويعزز قدرة الدول على الوفاء بالتزاماتها بموجب القانون الجنائي الدولي تجاه حماية البيانات والمعلومات الحساسة.

4-**تعمية البيانات:** تعمل على حماية البيانات أثناء النقل أو التخزين، ما يمنع استغلالها من قبل الجهات الإجرامية، ويضمن التزام الدول بالقواعد الدولية المتعلقة بسرية البيانات، ويعد هذا الإجراء أساسياً لدعم الأدلة الرقمية في المحاكم الدولية [(12)].

5- **تقنية المفتاح العام:** تُتيح هذه التقنية تقسيم البيانات على عدة خوادم مع استخدام مفاتيح تشفير معقدة، ما يحد من قدرة المهاجمين على الوصول إليها، ويُسهّل التزام الدول بالمعايير الجنائية الدولية في حماية المعلومات الرقمية ومنع الجرائم السيبرانية العابرة للحدود [(13)].

6-**الشبكة الافتراضية الخاصة** توفر هذه الشبكة بيئة محمية للتواصل بين المؤسسات المعنية بالأمن السيبراني، ما يضمن تنفيذ الإجراءات الجنائية الدولية بكفاءة، ويتيح تبادل المعلومات والتحقيقات مع الدول الأخرى في إطار اتفاقيات التعاون القضائي الدولي.

7-**تقنية الفجوة الهوائية (Air-gapping):** تُعزل البنية التحتية الحساسة عن الإنترنت العام، ما يقلل من خطر الاختراقات ويضمن حماية الأدلة الرقمية، ويتيح تطبيق العقوبات الجنائية الدولية على أي اعتداء على هذه البنية، كما يعزز مسؤولية الدول وفق القانون الدولي في تأمين المنشآت الحيوية [(14)].

[(10)] حامد محمد علي البلداوي، الهجمات السيبرانية أضرارها وآثارها ومواجهاتها في قواعد القانون الدولي الإنساني، مرجع سابق، ص137.

[(11)] ناصر العماش، الملتقى الوطني للأمن السيبراني، مقال منشور على الموقع الإلكتروني التالي: https://www.alriyadh.com/2003607، تاريخ الزيارة 2026/4/1.

[(12)] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، المرجع الإلكتروني السابق، ص 5.

[(13)] جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل مواجهتها، منشورات مكتبة السنهوري، بغداد، 2012، ص124.

[(14)] محمود الحمدان، الإرهاب الإلكتروني وسبل المواجهة، المرجع الإلكتروني السابق.

8-**مسجّل لوحة المفاتيح (Keylogger):** تُستخدم هذه التقنية لمراقبة نشاط الجهات الإجرامية وجمع الأدلة الرقمية، وهو ما يعزز قدرة السلطات القضائية على توجيه الملاحقات الجنائية وفق القانون الجنائي الدولي، ويضمن احترام القواعد القانونية عند جمع الأدلة الرقمية بما يضمن مقبوليتها أمام المحاكم الدولية.

9- **تقنية خلية العسل (Honey-cell) أو الطعم** تضمن هذه التقنية حماية البيانات واستعادتها بعد الهجمات السيبرانية، ما يعزز جمع الأدلة الرقمية وحفظها في شكل قانوني متوافق مع القانون الجنائي الدولي، ويُسهل متابعة التحقيقات الدولية وملاحقة الجناة بشكل فعال وموثق.

ويتضح من خلال ذلك أن تنظيم الضوابط والاستجابة لكل الإجراءات والمتغيرات، فضلاً عن التدريب والتوعية لجميع المستخدمين الذي سيرتقي بالبيئة السيبرانية إلى مراحل متقدمة نحو الوصول إلى الأهداف المرسومة، مشددًا على ضرورة تكاتف فرق العمل، سواء في الاجراءات الوطنية أم على مستوى الجهات الدولية، التي ستحقق النجاحات المأمولة في المجال السيبراني، وخلال ذلك تتمكن الجهات المعنية من مواجهة الإرهاب السيبراني إذا تمكنت من تحديد مفهومه بدقة، ثم تحديد أولوياتها في وضع إجراءات الحماية والمتابعة والتحقيق.

إن وجود رؤية واضحة لدى الجهات المختصة لهذا المفهوم يمكنها من تحديد الإجراءات اللازمة لمواجهة نشاطات الهجمات السيبرانية التي هي بين التدابير السياسية والتنظيمية التشريعية الفنية للإجراءات الوطنية، فضلاً عن التعاون الإقليمي والدولي في مجال الهجمات السيبرانية.

المطلب الثاني

الجريمة السيبرانية بين التشريعات الجنائية والقواعد الجنائية الدولية

إن إدخال أي تكنولوجيا جديدة إلى مجتمع من المجتمعات قد يؤدي إلى ظهور تحديات قانونية جديدة ضمن هذا المجتمع غير أنه من الممكن مع التطور التكنولوجي للمعلوماتية تطبيق التشريعات التقليدية التي تركز على الأشياء الملموسة ضمن حدود معينة على أن يصاحبها صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والأنظمة المعلوماتية، حيث يصعب تحديد صاحب أو الحائز على المعلومة ولاسيما على صعيد التجريم والاختصاص القضائي وإجراءات التحقيق والأدلة المعلوماتية[15]. **فبناءً على ذلك سنقسم هذا المطلب إلى فرعين، سنتناول في الفرع الأول انسجام القوانين الجنائية في الدول العربية مع المعايير الجنائية الدولية، وفي الفرع الثاني سنتناول توافق النظم العقابية في التشريعات الأجنبية مع قواعد القانون الجنائي الدولي.**

الفرع الأول

انسجام القوانين الجنائية في الدول العربية مع المعايير الجنائية الدولية

قطعت العديد من الدول العربية خطوات مهمة في مجال حماية الأمن السيبراني ومكافحة الإرهاب الإلكتروني الذي بات يشكل تهديداً حقيقياً للأمن القومي، وقد برزت الحاجة إلى تطوير التشريعات الوطنية لتواكب المستجدات التقنية والجرائم الحديثة، بما يتوافق مع المعايير الدولية لمكافحة الجرائم السيبرانية، بحيث يأتي هذا في سياق تعزيز التزامات الدول العربية بموجب الاتفاقيات الدولية، مثل اتفاقية بودابست لمكافحة الجرائم المعلوماتية، واتفاقيات الأمم المتحدة لمكافحة الإرهاب، بما يضمن حماية الأفراد والمؤسسات والممتلكات الرقمية على حد سواء، لذا اصدرت العديد من الدول العربية التشريعات

[15] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مركز المحمود لتوزيع الكتب القانونية، مصر، 2023، ص100.

والقوانين الوطنية لمكافحة مثل هذه الجريمة[16]، من أجل ضمان توفير الحماية القانونية الفاعلة للأفراد وللمؤسسات الحكومية والخاصة من هذه الجرائم، لذلك سنتناول هذه التشريعات كل على حدة على الشكل التالي:

أولاً–التشريع العراقي:

في العراق أدركت السلطات العراقية أن هناك أثر للفضاء السيبراني على الأمن الوطني خاصة بعد أحداث 11 سبتمبر 2001، حيث أصبحت الجماعات الإرهابية قادرة على استغلال التقنيات الحديثة في تنفيذ هجماتها ومن أجل مواجهة مثل هذه المخاطر فقد اعتمد العراق عدة تشريعات وطنية تتعلق بالجرائم الإلكترونية، لذلك سوف نتطرق إلى بعض القوانين العراقية لمواجهة الجرائم الإلكترونية، كالتالي[17]:

1–**قانون العقوبات العراقي رقم (111) لسنة 1969:** يعتبر قانون العقوبات العراقي رقم 111 لسنة 1969 أن جرائم الاعتداء على وسائل الاتصالات السلكية واللاسلكية هي من الجرائم ذات الخطر العام المضر بالمصلحة العامة، لذلك فقد عاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس من عطل عمداً وسيلة من وسائل الاتصال السلكي أو اللاسلكية المختصة لمنفعة عامة أو قطع أو تلغي شيئًا من أسلاكها أو أجهزتها أو حال عمدًا دون اصلاحها. وتكون العقوبة بالسجن اذا ارتكب الجريمة باستعمال مواد مفرقعة أو متفجرة، اذا ارتكب في وقت حرب أو فتنته أو هياج[18].

2–**قانون مكافحة الإرهاب رقم 13 لسنة 2005:** لم ينص هذا القانون على مكافحة الجرائم الإلكترونية، ولكنه عرف الإرهاب في مادته الأولى بأنه:" كل فعل إجرامي يقوم به الفرد أو جماعة منظمة استهدف فردًا أو مجموعة أفراد أو جماعات أو مؤسسات رسمية أو غير رسمية أوقع الأضرار بالممتلكات العامة أو الخاصة بغية الإخلال بالوضع الأمني أو الاستقرار والوحدة الوطنية أو إدخال الرعب والخوف والفزع بين الناس أو إثارة الفوضى تحقيقاً لغايات إرهابية"[19].

3–**مشروع قانون الجريمة المعلوماتية لسنة 2018:** خلال البحث الذي قمنا به توافرت لدينا معلومات عن شروع مجلس النواب العراقي بإعداد مشروع قانون خاص بالجريمة المعلوماتية، الذي حدد في المادة (2) منه أهم الأهداف التي يسعى إلى تحقيقها[20]، كما أصدر برلمان كردستان العراق بتاريخ 19/5/2008 قانوناً، وهو يتألف من ثمانية مواد بالإضافة الى أسبابه الموجبة، وبذلك يكون هذا القانون ساير أغلب القوانين منها قانون إقليم كردستان خصوصاً[21]،هذا التشريع يتيح إمكانية التعاون مع المحاكم الدولية واستعمال الأدلة الرقمية في إطار القانون الجنائي الدولي.

ثالثاً–التشريع اللبناني:

بذل لبنان جهوداً ملموسة في مجال مكافحة تهديدات الإرهاب الإلكتروني، ومنها إنشاء الهيئة الناظمة للاتصالات في عام 2007، والتي أصبحت عضواً فاعلاً في الشراكة الدولية المتعددة الأطراف لمكافحة التهديدات والهجمات السيبرانية، فضلاً

---

[16] علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، 2019، ص234.

[17] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت دار المطبوعات الجامعية، الإسكندرية، مصر، 2018، ص237.

[18] المادة (361) من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.

[19] المادة (1) من قانون مكافحة الإرهاب رقم 13 لسنة 2005 النافذ.

[20] نص مشروع قانون الجريمة المعلوماتية العراقي لسنة 2018 على: أ– توفير الحماية القانونية للاستخدام الاستخدام المشروع للحاسب وشبكة المعلومات، ب – تحقيق الأمن المعلوماتي وتوفير اقصى درجات ممكنة من الحماية لشبكات المعلومات وأجهزة الحاسوب وبرامج الحاسوب من الاعتداءات وسوء الاستخدام والهجوم الالكتروني، ج– معاقبة مرتكبي جرائم المعلومات، د– حفظ الحقوق على الاستخدام القانوني المشروع للحاسبات والشبكات المعلوماتية، هـ– حماية المصلحة العامة والأخلاق والآداب العامة، و–حماية الاقتصاد الوطني.

[21] مازن ليلو راضي، وعدي سليمان علي، المواجهة التشريعية للجريمة الإلكترونية في إقليم كردستان العراق، بحث منشور في مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الأول لكلية القانون، مجموعة 2، العراق، 2009، ص 49.

عن إقرار قانون التنصت رقم (140)، وقانون حقوق الملكية الفكرية رقم (75)، هذا فضلاً عن إنشاء مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية التابع لقسم المباحث الجنائية الخاصة، ضمن وحدة الشرطة القضائية في المديرية العامة لقوى الأمن الداخلي، وتتمثل مهمة هذا المكتب في مكافحة الجرائم التي تستخدم فيها التقنيات المعلوماتية العالية، وجرائم التعدي على الملكية الفكرية[22].

الفرع الثاني

توافق النظم العقابية في التشريعات الأجنبية مع قواعد القانون الجنائي الدولي

إن مواجهة الجرائم السيبرانية قد أصبحت أمراً حيوياً في العالم المعاصر ومع تطور التكنولوجيا بشكل سريع مما أدى إلى زيادة التهديدات السيبرانية، تشمل هذه التهديدات الاختراقات الإلكترونية، والاحتيال الإلكتروني وسرقة البيانات والاختراقات الهجومية على الأنظمة الحيوية للدول مما يستدعي تنفيذ تشريعات عقابية فعّالة لمكافحة هذه الجرائم، ومواءمة التشريعات العقابية الأجنبية في مجال مكافحة الجرائم السيبرانية تتضمن مجموعة من الجهود والآليات التي تهدف إلى تعزيز التعاون الدولي وتعزيز قدرة الدول على مكافحة الجرائم السيبرانية عبر الحدود، من بين أهم الدول في هذا السياق هي التالية:

أولاً_ فرنسا

جعلت فرنسا الأمن السيبراني من أولوياتها منذ العقد الأول من القرن الحادي والعشرين، ودفعت عودة التهديد الإرهابي عام 2015 إلى تكثيف جهودها في هذا المجال، وقد حددت الاستراتيجية الوطنية للأمن الرقمي خمسة أهداف[23]، وهي ضمان السيادة الوطنية، والرد على الأعمال الخبيثة السيبرانية، وإعلام الجمهور العام، وجعل الأمن الرقمي ميزة تنافسية للشركات، وتقوية صوت فرنسا دولياً، وتؤخذ الجرائم الإلكترونية في الاعتبار قانونياً منذ قانون حماية البيانات (نافذة جديدة) منذ عام (1978) الذي ينظم حرية ابداع الأشخاص، واليوم تخضع الممارسات الرقمية لنظام قانوني ينص على عقوبات تصل إلى السجن لمدة خمس سنوات وغرامة قدرها 75000 يورو على هجمات الكمبيوتر، كما ينص القانون على زيادة العقوبات على الهجمات الإلكترونية التي تستهدف الدولة بشكل مباشر، وفي عام 2009 تم انشاء وكالة أمن نظم المعلومات الوطنية (نافذة جديدة) للدفاع عن أنظمة المعلومات والمستخدمين الرقميين وحمايتهم من الهجمات الإلكترونية مهامها هي كما يلي مراقبة الشبكات لاكتشاف الهجمات والسماح بالرد بأسرع ما يمكن، تطوير منتجات وخدمات الأمن السيبراني للمستخدمين، تقديم الخبرة والمساعدة للإدارات والشركات، توعية الجمهور بشأن التهديدات السيبرانية.

وفي عام 2017 أطلقت الحكومة نظاماً وطنياً لمساعدة ضحايا الأعمال الإجرامية الإلكترونية احتضنته باريس وشارك في تجريبه مع وزارة الداخلية، منصة cybermalveillance.gouv.fr (نافذة جديدة) يربط ضحايا الهجمات الإلكترونية، الأفراد أو الشركات أو السلطات المحلية، ومقدمي الخدمات الذين من المحتمل أن يساعدوهم في جهودهم كما أعيد تصميم النظام الأساسي في أوائل عام 2020، وشهدت زيادة بنسبة 155 في حركة المرور[24].

كما إن الاستراتيجية الرقمية الدولية لفرنسا التي قدمها وزير أوروبا والشؤون الخارجية في ديسمبر 2017 يلخص جميع التوجهات الاستراتيجية التي تروج لها فرنسا في العالم الرقمي حول ثلاث ركائز الحوكمة، والاقتصاد، والأمن، ثم تم إنشاء

---

[22] روني حداد، الإرهاب الإلكتروني وتحديات مواجهته، مجلة الجيش، العدد394، بيروت، 2018، ص2.

[23] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مرجع سابق، ص108.

[24] طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي والمعاصر، بحث منشور في مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، الأردن، 2019، ص84.

الوكالة الوطنية لأمن أنظمة المعلومات (ANSSI) في عام 2009، وهي السلطة الوطنية المعنية بالأمن السيبراني، بصفته "رجل إطفاء" حقيقي للفضاء الإلكتروني الفرنسي فهو مسؤول عن الوقاية (بما في ذلك من حيث المعايير) والاستجابة لحوادث الكمبيوتر التي تستهدف المؤسسات الحساسة، كما إنه ينظم تدريبات على إدارة الأزمات على المستوى الوطني توظف ANSSI الآن 600 شخص وتستمر في النمو[25].

أما وزارة القوات المسلحة فإن لديها مهمة مزدوجة تتمثل في ضمان حماية الشبكات التي تدعم عملها ودمج القتال الرقمي في قلب العمليات العسكرية من أجل تعزيز عمل الوزارة في هذا المجال، لذلك قد تم إنشاء قيادة الدفاع الإلكتروني (COMCYBER) بموجب أوامر من رئيس أركان الدفاع، في أوائل عام 2017[26]، تتمثل مهمة وزارة الداخلية في مكافحة جميع أشكال الجرائم الإلكترونية واستهداف المؤسسات والمصالح الوطنية، واللاعبين الاقتصاديين والهيئات العامة وكذلك الأفراد، وتحقيقاً لهذه الغاية تم حشد الأجهزة المركزية المتخصصة والشبكات الإقليمية للشرطة الوطنية والدرك الوطني والأمن الداخلي، وهم مسؤولون عن التحقيقات التي تهدف إلى تحديد مرتكبي الأفعال الكيدية السيبرانية وتقديمهم إلى العدالة، كما تساهم هذه الخدمات في الوقاية ورفع مستوى الوعي لدى الجمهور المعني.

1- **أمن نظم المعلومات (ISS) والكتاب الأبيض للدفاع والأمن القومي لعام 2008:** هذا الكتاب الأبيض، الذي يحتفظ بخطر هجوم الكمبيوتر على البنى التحتية الوطنية كواحد من أكثر التهديدات الرئيسية المحتملة على مدار الخمسة عشر عاماً القادمة، يسلط الضوء على التأثير القوي المحتمل لمثل هذه الهجمات على حياة الأمة، إن اعتمادنا على عمليات تكنولوجيا المعلومات يتزايد باستمرار مع تطور مجتمع المعلومات والاستخدام المتزايد لتكنولوجيا المعلومات في العمليات الأساسية للدولة والمجتمع[27]، وبناءً على ذلك فقد دعا الكتاب الأبيض الدولة إلى تزويد نفسها بالقدرة على منع الهجمات الحاسوبية والرد عليها، ولجعل ذلك أولوية رئيسية لنظام الأمن القومي لديها على وجه الخصوص، في مجال الدفاع عن أنظمة المعلومات، شدد على الحاجة إلى امتلاك القدرة على الكشف المبكر عن هجمات الكمبيوتر، ووجود منظمة قادرة على مواجهة الهجمات الأكثر دقة بالإضافة إلى الهجمات الأكثر ضخامة وفي مجال الوقاية، فقد اقترحت زيادة استخدام المنتجات والشبكات الأمنية العالية المستوى، وإنشاء مستودع من المهارات لفائدة إدارات ومشغلي البنى التحتية الحيوية[28]، وقد تم إنشاء ANSSI وفقاً للإرشادات الواردة في هذا الكتاب الأبيض بشأن الدفاع والأمن القومي من أجل اقتراح الاستراتيجية الوطنية لأمن نظم المعلومات حيث تم تشكيل لجنة استراتيجية ISS بموجب المرسوم المنشئ لـ ANSSIK بالإضافة إلى إنشاءANSSI، يوفر هذا المستند التعريفي التمهيدي إنشاء مرصد أمن لأنظمة المعلومات (OzSSI) على مستوى كل منطقة دفاع وأمن تتمثل مهمة هذه المراصد في نقل الإجراءات المتخذة لتحسين أمن نظم المعلومات في جميع أنحاء الأراضي الوطنية.

2-**الكتاب الأبيض لعام 2013 حول الدفاع والأمن القومي وLPM[29]**: في عام 2013، استجابة لملاحظة الزيادة في كمية وتعقيد الهجمات الإلكترونية ضد أنظمة المعلومات للعديد من الشركات الوطنية والحكومية حيث تم نشر كتاب أبيض

---

[25] ايهاب خليفة، القوة الالكترونية كيف يمكن ان تدير الدول شؤنها في عصر الانترنيت، المركز العربي للنشر والتوزيع، مصر، 2017، ص254.

[26] طلال ياسين العيسى، عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي والمعاصر، مرجع سابق، ص234.

[27] ايهاب خليفة، الحرب السيبرانية مراجعة العقيدة العسكرية استعداداً للمعركة القادمة، مقال منشور في مجلة السياسة الدولية، العدد 211، مصر، 2018، ص 20.

[28] سامر عبد اللطيف، الحرب في الفضاء الرقمي (رؤية مستقبلية)، بحث منشور في مجلة رسالة الحقوق، جامعة كربلاء، السنة السابعة، العدد الثاني، العراق، 2015، ص96.

[29] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مرجع سابق، ص111.

جديد، إنه يمثل نقطة تحول لم تعد الدولة راضية عن تلبية احتياجاتها الخاصة بالأمن السيبراني، ولكنها الآن تأخذ في الاعتبار احتياجات المشغلين الحيوية للأمة وفي 19 ديسمبر 2013 صدر القانون رقم 2013/1168 بشأن البرمجة العسكرية (LPM) يتبع المبادئ التوجيهية التي حددها الكتاب الأبيض لعام 2013 بشأن الدفاع والأمن القومي. إنها الأداة التشريعية التي ستسمح للمشغلين من القطاعين العام والخاص المهمين للأمة لحماية نفسها بشكل أفضل ولـ ANSSI – وخدمات الدولة الأخرى – لدعمها بشكل أفضل في حالة وقوع هجوم على الكمبيوتر، وتنص المادة (22) منه على اعتماد تدابير لتعزيز سلامة المشغلين ذوي الأهمية الحيوية ومنح صلاحيات جديدة لرئيس الوزراء[30]، كما تمتلك فرنسا أيضًا شبكة من CERTS، والمنظمات الرسمية المسؤولة عن تقديم خدمات الوقاية من المخاطر والمساعدة في التعامل مع الحوادث، هذه CERTS (فريق استجابة طوارئ الكمبيوتر) هي مراكز للتنبيه والرد على هجمات الكمبيوتر، وهي مخصصة للشركات أو الإدارات، وهي من المعلومات التي يمكن للجميع الوصول إليها بشكل عام.

ثالثاً–الولايات المتحدة الامريكية:

تأتي الولايات المتحدة الأمريكية في مقدمة الدول التي واجهت الجرائم المعلوماتية، وذلك بالنص على مواجهتها تشريعياً حتى يعطى للفعل وصف الجريمة، وقد تم إنشاء إدارة متخصصة لمتابعة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالي (FBI) يضم داخله مجموعة من الأفراد المدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والحفاظ على ما يتم تحصيله من أدلة، تتحدد اختصاصات إدارة مكافحة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالي وفقاً لما يلي[31]:

1–عند تلقى الإخطار بوقوع الجريمة يتم الانتقال إلى مكان ارتكاب الجريمة ثم يقوموا بالحصول على كافة المعلومات عن أسلوب العمل والذي يمكنه أن يعين في كشف الجريمة وتحديد شخص مرتكبيها.

2– يقوم الفريق المكلف بالبحث والتحري بتنظيم العمل داخله من خلال الآتي: أ– تنظيم عملية الاتصال بين الأعضاء المختلفين للفريق ولذلك تبدأ عملية الاتصال قبل بدء عملية البحث. ب–يتم وضع خطة بحثية مكتوبة توضح بالتفصيل كافة الأنشطة البحثية المتوقعة ويحدد فيها دور كل فرد بالفريق وكيفية التنسيق فيما بينهم. ج–يقوم الفريق بعملية البحث في الأنواع المختلفة من السجلات والتسجيلات التي لها صلة بالقضية والتي تتضمن بعض المعلومات الهامة مثل توثيق نظام الكمبيوتر ومعلومات تشغيله[32].

3_ يتم الاستعانة بعملية المراقبة لتحديد الشخص المشتبه فيه إذا كان هذا الشخص من داخل المؤسسة أو المنشأة وذلك عن طريق الاستعانة بمجموعة من البرامج عالية الكفاءة في اكتشاف مرتكب الجريمة.

4– يتم تسجيل كافة المعلومات التي يتم العثور عليها في أي من الوسائط المتعددة أو في وحدات التسجيل الداخلية عند بداية ونهاية التحريات لإثبات عدم التسبب في حدوث أي تلف لأي من الأدلة[33].

هكذا جاءت السياسات الوطنية لترد على المنظمات العقابية المعاصرة للرد على الجريمة السيبرانية.

---

[30] نص المادة (22) من الكتاب الأبيض الفرنسي لعام 2013 حول الدفاع والأمن القومي وLPM.

[31] سعد عاطف عبد المطلب، دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي–دراسة مقارنة، بحث منشور في مجلة كلية الآداب، مصر، 2019، ص 526.

[32] إسماعيل محمود الرزاز، الحماية القانونية من الهجمات والجرائم السيبرانية، مرجع سابق، ص113.

[33] سامر عبد اللطيف، الحرب في الفضاء الرقمي (رؤية مستقبلية)، مرجع سابق، ص99.

الخاتمة

تظهر دراسة الجريمة السيبرانية بين السياسات الوطنية والمنظمات العقابية أن العالم يشهد تحولاً نوعياً في طبيعة الجريمة حيث لم تعد مقيدة بحدود جغرافية أو أدوات تقليدية، بل أصبحت قائمة على بيئة رقمية متغيرة ومعقدة، تتطلب استجابات قانونية ومؤسسية متطورة، وقد كشفت الدراسة أن السياسات الوطنية رغم ما شهدته من تطور ملحوظ في العديد من الدول، ما زالت تواجه تحديات حقيقية في مواكبة السرعة الهائلة للتطور التقني، الأمر الذي ينعكس على قدرتها في تحقيق الردع الفعال كما تبين أن المنظمات العقابية، سواء على المستوى الوطني أو الدولي، تضطلع بدور مهم في مكافحة هذه الجرائم غير أن هذا الدور لا يزال مقيداً بإشكاليات التعاون الدولي، وتباين الأنظمة القانونية وصعوبات الإثبات الرقمي.

وفي ضوء ذلك فإن مواجهة الجريمة السيبرانية تقتضي اعتماد مقاربة شاملة تقوم على التكامل بين التشريع والتقنية والتعاون الدولي، بما يضمن تحقيق التوازن بين حماية المجتمع وضمان الحقوق والحريات، ويعزز من فعالية العدالة الجنائية في البيئة الرقمية.

أولاً_ الاستنتاجات

1. إن الجريمة السيبرانية تتميز بطبيعة عابرة للحدود، مما يجعل مواجهتها من خلال السياسات الوطنية وحدها أمراً غير كافٍ دون وجود تعاون دولي فعال.
2. تعاني العديد من التشريعات الوطنية من قصور في مواكبة التطور التكنولوجي، سواء من حيث التجريم أو من حيث وسائل الإثبات والإجراءات.
3. تواجه المنظمات العقابية صعوبات كبيرة في ملاحقة مرتكبي الجرائم السيبرانية بسبب إشكاليات الاختصاص القضائي وتعدد النظم القانونية.
4. يشكل الإثبات الرقمي أحد أبرز التحديات في مكافحة الجريمة السيبرانية، نظراً لتعقيد الأدلة وسهولة إتلافها أو إخفائها.
5. إن ضعف التنسيق بين الجهات الوطنية والدولية يحد من فعالية الجهود المبذولة في مكافحة الجرائم السيبرانية ويؤدي إلى إفلات بعض الجناة من العقاب.

ثانياً_ المقترحات

1. العمل على تحديث التشريعات الوطنية بشكل دوري لتواكب التطورات التقنية المتسارعة، مع إدراج نصوص خاصة بالجرائم السيبرانية.
2. تعزيز التعاون الدولي من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة وتفعيل آليات المساعدة القانونية المتبادلة.
3. إنشاء وحدات متخصصة داخل الأجهزة القضائية والأمنية مزودة بالخبرات التقنية اللازمة للتعامل مع الجرائم السيبرانية.
4. تطوير آليات الإثبات الرقمي واعتماد وسائل تقنية حديثة تضمن جمع الأدلة وحفظها بشكل قانوني سليم.
5. نشر الوعي المجتمعي بمخاطر الجريمة السيبرانية وسبل الوقاية منها، بما يسهم في الحد من انتشارها وتعزيز الأمن الرقمي.

قائمة المصادر والمراجع

أولاً: الكتب

1. أمير فرج يوسف .(2008) .**الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت** .مصر: مكتبة الوفاء القانونية.

Youssef, Amir Farag. (2008). **Electronic and Informational Crime and International and Local Efforts to Combat Computer and Internet Crimes**. Egypt: Al-Wafa Legal Library.

2. حامد محمد علي البلداوي .(2024) .**الهجمات السيبرانية: أضرارها وآثارها ومواجهتها في قواعد القانون الدولي الإنساني** .القاهرة: المركز العربي.

Al-Baldawi, Hamed Mohammed Ali. (2024). **Cyberattacks: Their Damages, Effects, and Confrontation under the Rules of International Humanitarian Law**. Cairo: Arab Center.

3. عادل عبد العال إبراهيم خراشي .(2015) .**إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها** .الإسكندرية، مصر: دار الجامعة الجديدة.

Kharashi, Adel Abdel Aal Ibrahim. (2015). **Problems of International Cooperation in Combating Information Crimes and Ways to Overcome Them**. Alexandria, Egypt: Dar Al-Jami'a Al-Jadida.

4. جمال إبراهيم الحيدري .(2012) .**الجرائم الإلكترونية وسبل مواجهتها** .بغداد: منشورات مكتبة السنهوري.

Al-Haidari, Jamal Ibrahim. (2012). **Cybercrimes and Ways to Confront Them**. Baghdad: Al-Sanhouri Library Publications.

5. إسماعيل محمود الرزاز .(2023) .**الحماية القانونية من الهجمات والجرائم السيبرانية** .مصر: مركز المحمود لتوزيع الكتب القانونية.

Al-Razzaz, Ismail Mahmoud. (2023). **Legal Protection against Cyberattacks and Cybercrimes**. Egypt: Al-Mahmoud Center for Legal Book Distribution.

6. علي محمد كاظم الموسوي .(2019) .**المشاركة المباشرة في الهجمات السيبرانية** .بيروت: المؤسسة الحديثة للكتاب.

Al-Moussawi, Ali Mohammed Kazem. (2019). **Direct Participation in Cyberattacks**. Beirut: Modern Book Foundation.

7. محمد أمين الرومي .(2018) .**جرائم الكمبيوتر والإنترنت** .الإسكندرية، مصر: دار المطبوعات الجامعية.

Al-Roumi, Mohammed Amin. (2018). **Computer and Internet Crimes**. Alexandria, Egypt: University Publications House.

8. روني حداد .(2018) .**الإرهاب الإلكتروني وتحديات مواجهته** .مجلة الجيش، العدد 394، بيروت.

Haddad, Rony. (2018). **Cyberterrorism and the Challenges of Confronting It**. *Army Magazine*, Issue 394, Beirut.

9. إيهاب خليفة .(2017) .**القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت** .مصر: المركز العربي للنشر والتوزيع.

Khalifa, Ehab. (2017). **Electronic Power: How States Can Manage Their Affairs in the Age of the Internet**. Egypt: Arab Center for Publishing and Distribution.

ثانياً: الأطاريح

1. أحمد سعد محمد الحسيني .(2012) .**الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية** .أطروحة دكتوراه في القانون العام، جامعة عين شمس، مصر.

Al-Husseini, Ahmed Saad Mohammed. (2012). **Procedural Aspects of Crimes Arising from the Use of Electronic Networks**. PhD Dissertation in Public Law, Ain Shams University, Egypt.

2. درار نسيمة .(2017) .**الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني** .أطروحة دكتوراه في القانون العام، جامعة أبو بكر بلقايد، الجزائر.

Derar, Nassima. (2017). **Information Security and Ways to Confront Its Risks in Electronic Transactions**. PhD Dissertation in Public Law, Abou Bekr Belkaid University, Algeria.

ثالثاً: المجلات والدوريات

1. مازن ليلو راضي، وعدي سليمان علي .(2009) .**المواجهة التشريعية للجريمة الإلكترونية في إقليم كردستان العراق** . مجلة جامعة تكريت للعلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الأول لكلية القانون، المجموعة الثانية، العراق.

Radhi, Mazen Lilo, & Ali, Uday Suleiman. (2009). **Legislative Confrontation of Cybercrime in the Kurdistan Region of Iraq**. *Tikrit University Journal of Legal and Political Sciences*, Special Issue of the First Scientific Conference of the College of Law, Group 2, Iraq.

2. طلال ياسين العيسى، وعدي محمد عناب .(2019) .**المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي والمعاصر** .مجلة الزرقاء للبحوث والدراسات الإنسانية، 19(1)، الأردن.

Al-Issa, Talal Yassin, & Annab, Uday Mohammed. (2019). **International Responsibility Arising from Cyberattacks in Light of Contemporary International Law**. *Zarqa Journal for Research and Human Studies*, 19(1), Jordan.

3. إيهاب خليفة .(2018) .**الحرب السيبرانية: مراجعة العقيدة العسكرية استعداداً للمعركة القادمة** .مجلة السياسة الدولية، العدد 211، مصر.

Khalifa, Ehab. (2018). **Cyber Warfare: Reviewing Military Doctrine in Preparation for the Coming Battle**. *International Politics Journal*, Issue 211, Egypt.

4. سامر عبد اللطيف .(2015) .**الحرب في الفضاء الرقمي: رؤية مستقبلية** .مجلة رسالة الحقوق، جامعة كربلاء، السنة السابعة، العدد الثاني، العراق.

Abdel Latif, Samer. (2015). **War in Digital Space: A Future Vision**. *Risalat Al-Huquq Journal*, University of Karbala, 7th Year, Issue 2, Iraq.

5. سعد عاطف عبد المطلب .(2019) .**دور الشرطة في مكافحة الجرائم السيبرانية المستحدثة وتحقيق الأمن المعلوماتي: دراسة مقارنة** .مجلة كلية الآداب، مصر.

Abdel Muttalib, Saad Atef. (2019). **The Role of the Police in Combating Emerging Cybercrimes and Achieving Information Security: A Comparative Study**. *Journal of the Faculty of Arts*, Egypt.

رابعاً: القوانين والوثائق الرسمية

1. **قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.**

Iraqi Penal Code No. 111 of 1969, as amended.

2. **قانون مكافحة الإرهاب العراقي رقم 13 لسنة 2005 النافذ.**

Iraqi Anti-Terrorism Law No. 13 of 2005, in force.

3. **الكتاب الأبيض الفرنسي لعام 2013 حول الدفاع والأمن القومي وقانون البرمجة العسكرية.LPM**

The French White Paper of 2013 on Defense and National Security and the Military Programming Law (LPM).

خامساً: المراجع الإلكترونية

1. محمود الحمدان. (2021، 21 يناير) .**الإرهاب الإلكتروني وسبل المواجهة** .منشور على موقع التحالف الإسلامي العسكري لمحاربة الإرهاب. تاريخ الزيارة: 1-5-2025.

Al-Hamdan, Mahmoud. (2021, January 21). **Cyberterrorism and Ways to Confront It**. Published on the website of the Islamic Military Counter Terrorism Coalition. Accessed: 1 May 2025.

2. ناصر العماش .**الملتقى الوطني للأمن السيبراني** .منشور على موقع جريدة الرياض.

Al-Ammash, Nasser. **The National Forum for Cybersecurity**. Published on Al-Riyadh Newspaper website.